ORIGINAL

Before the

Federal Communications Commission

DOCKET FILE COPY ORIGINAL

Washington, D.C. 20554

RECEIVED

DEC 12 1997

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of	)	
	)	
Communications Assistance for	)	CC Docket No. 97-213
Law Enforcement Act	)	

COMMENTS OF AIRTOUCH COMMUNICATIONS, INC.

AIRTOUCH COMMUNICATIONS, INC.

Kathleen Q. Abernathy
David A. Gross
Donna L. Bethea
AirTouch Communications, Inc.
1818 N Street, N.W.
Washington, D.C. 20036
(202) 293-3800

December 12, 1997

Table of Contents

Before the

Federal Communications Commission

Washington, D.C. 20554

In the Matter of	)	
	)	
Communications Assistance for	)	CC Docket No. 97-213
Law Enforcement Act	)	

COMMENTS OF AIRTOUCH COMMUNICATIONS, INC.

AirTouch Communications, Inc. ("AirTouch") provides the following comments in response to the *Notice of Proposed Rulemaking*,[1] wherein the Commission seeks to implement the Communications Assistance for Law Enforcement Act ("CALEA").[2] AirTouch has ownership interests in numerous broadband and narrowband commercial mobile radio service ("CMRS") systems in the United States and 11 other countries, in addition to the new Globalstar mobile satellite system.[3]

AirTouch has a keen interest in this proceeding. It is committed to continue supporting fully the legitimate needs of law enforcement. At the same time, AirTouch wants to ensure that it can implement CALEA in a way that protects fully the privacy rights of its

---

1 *Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, *Notice of Proposed Rulemaking*, FCC 97-356 (Oct. 10, 1997), *Errata* (Oct. 24, 1996)("*CALEA NPRM*").

2 Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994), *codified in* various sections of titles 18 and 47 of the United States Code, including 47 U.S.C. §§ 229 and 1001-10.

3 Based in San Jose, California, Globalstar is a limited partnership company formed in 1991 by a consortium of the world's leading telecommunications companies to develop, launch, and operate the Globalstar low-earth-orbit satellite communications system.

customers and in a way that is most cost effective, so that needless costs are not imposed on consumers or the federal government (in connection with its CALEA reimbursement obligations).

INTRODUCTION AND SUMMARY

The telecommunications industry will be unable to meet CALEA's requirements on the current October 25, 1998 compliance date. This situation has not been caused by the industry; to the contrary, as documented in Part I below, the industry has fully attempted to find solutions which meet CALEA's requirements and law enforcement's needs. However, the FBI and industry have been for some time at a stalemate over what features and capabilities are, and are not, required by CALEA. Congress expressly charged this Commission with resolving these types of disputes, and on July 16, 1997 CTIA submitted a petition requesting the Commission to intervene to resolve these matters. AirTouch encourages the Commission to act swiftly on the CTIA petition. The sooner the Commission acts, the sooner vendors can develop CALEA-complaint equipment, the sooner carriers can install and test necessary CALEA modifications to their networks, and the sooner carriers can discharge their statutory responsibilities under CALEA.

The industry and FBI have conducted extensive discussions since CALEA was enacted. These discussions have, not surprisingly, focused on interception implementation issues pertaining to the networks which will effectuate most interceptions: landline and cellular/broadband PCS. However, the FBI has been so overwhelmed with the numerous issues related to those networks that it has been unable to address the unique implementation issues faced by mobile satellite and paging carriers. AirTouch identifies some of these unique issues

and reaffirms its commitment to work with the FBI concerning CALEA implementation in mobile satellite and paging networks once the FBI is ready to proceed in these areas.

The Commission, largely at the recommendation of the FBI, has proposed detailed recordkeeping rules concerning CALEA compliance. Such pervasive regulation is not only unnecessary, but it would also have the unintended effect of imposing needless costs on carriers and their customers. It bears remembering that the industry has successfully effectuated over the past three decades thousands of interceptions *without* extensive regulations of the type now proposed. In Part II below, AirTouch makes specific suggestions regarding how the Commission can streamline the FBI's proposed recordkeeping proposals so governmental interests are served without contravening the requirements of the Paperwork Reduction Act.

Finally, AirTouch recommends that the Commission decline the FBI's invitation to interpret various provisions of the 1968 Wiretap Act. The Wiretap Act was enacted nearly 30 years ago and there is much available precedent. Further, Courts would be under no obligation to follow the Commission interpretations in any event, and AirTouch submits that the Commission's limited resources could be better utilized by addressing the many other CALEA implementation issues in need of resolution which squarely fall within the Commission's jurisdiction.

DISCUSSION

I. The Commission Should Broaden this Proceeding to Include the Critically Important Standards and Compliance Deadline Issues

The telecommunications industry will be unable to comply with CALEA's requirements on the scheduled October 25, 1998 compliance date. This situation has not been caused by the industry; to the contrary, as documented in subpart A below, the industry has fully

attempted to negotiate with the FBI so that CALEA's requirements could be timely implemented. Regardless of the reasons for the current situation, the fact is that the FBI and the industry are, and have been for some time, at a stalemate. This impasse will not likely be broken without the Commission's active intervention, and the longer the Commission waits to intervene, the longer it will be before CALEA can be implemented.

A. CALEA Has Not Been Implemented As Congress Envisioned

Despite the best efforts of the telecommunications industry, CALEA has not been implemented in the manner Congress envisioned. Indeed, even the FBI acknowledged during a November 14, 1997 meeting with industry that CALEA's current compliance date of October 25, 1998 cannot now be met.

CALEA was enacted "to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes."[4] CALEA imposes on carriers two different law enforcement "assistance" obligations:

1. A *capability* requirement, wherein carriers are required to provide four interception capabilities to law enforcement;[5] and

2. A *capacity* requirement, wherein carriers are required under certain circumstances to provide these capabilities in quantities which the government specifies.[6]

---

4 H.R. Rep. No. 103-827, at 1 (1994)("House Report").

5 CALEA § 103(a)(1)-(4), *codified at* 47 U.S.C. § 1002(a)(1)-(4). With respect to these capability requirements, Congress made clear that CALEA is "intended to preserve the status quo, and that it [is] intended to provide law enforcement no more and no less access to information than [law enforcement] had in the past." House Report, *supra,* note 4 at 22-23.

6 *CALEA* § 104(b), *codified at* 47 U.S.C. § 1003(b). Importantly, carriers are under no

(continued...)

Although CALEA became effective on October 25, 1994, Congress decided that the capability and capacity requirements should not become effective for four years (*i.e.,* by October 25, 1998) "to ease the burden on [the] industry."[7]

CALEA's capacity and capability requirements are inextricably interrelated. The manner in which a carrier and its vendors meet the specified capability requirements will depend heavily on the extent of the government's capacity needs. Thus, capacity and capability should be planned for and developed concurrently to take advantage of design and scale efficiencies.

Congress directed the FBI to publish its capacity requirements within one year (by October 25, 1995) — "after notice and comment" and "after consulting with . . . telecommunications carriers."[8] Congress thus expected that carriers would have three years in which to meet the published capacity requirements (from October 25, 1995 to October 25, 1998).[9] The expected early publication of the FBI capacity requirements was also intended to give carriers and their vendors ample opportunity to consider the FBI's capacity needs in engineering cost-effective solutions for satisfying the capability requirements.

Further, with respect to the capability requirements, Congress determined that "the telecommunications industry itself shall decide how to implement law enforcement's

---

6 (...continued)
obligation to expand their capacity to meet government requirements *unless* the FBI agrees to "reimburse a carrier for costs directly associated with modifications to attain such capacity requirements that are determined to be reasonable." *Id.* § 104(e), *codified at* 47 U.S.C. § 1003(e). *See CALEA NPRM* ¶ 47.

7 *See* House Report, *supra,* note 4 at 18.

8 CALEA § 104(a)(1), *codified at* 47 U.S.C. § 1003(a)(1).

9 CALEA § 104(b)(1), *codified at* 47 U.S.C. § 1003(b)(1).

requirements."[10] Specifically, Congress envisioned that accredited industry organizations would develop necessary implementation standards "[t]o ensure the efficient and industry-wide implementation of the assistance capability requirements."[11] In addition, Congress specifically included a "safe harbor" provision so that carriers will be deemed "in compliance with the assistance capability requirements" if they are "in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization."[12]

Finally, Congress gave to the Commission important implementation authority. First, to ensure that the adoption of necessary technical standards is not delayed unreasonably, Congress empowered the Commission to establish such requirements if industry associations "fail to issue technical requirements or standards *or* if a Government agency or any other person believes that such requirements or standards are deficient."[13] Congress also authorized the Commission to extend the October 1998 compliance date if "compliance with the assistance

---

10 House Report, *supra*, note 4 at 19. Indeed, Congress expressly *prohibited* law enforcement agencies from requiring carriers to adopt "any specific design of equipment, facilities, services, features, or system configuration." CALEA § 103(b)(1), *codified at* 47 U.S.C. § 1002(b)(1).

11 CALEA § 107(a)(1), *codified at* 47 U.S.C. § 1006(a)(1). The importance of industry standards for CALEA implementation is apparent. As TIA's president recently advised Congress, it would be "foolhardy" for a manufacturer to "begin designing a set of features as complex as CALEA without an industry standard. Not only would it be prohibitively expensive (requiring great engineering resources from each manufacturer), but it could also result in serious incompatibilities in various manufacturers' architectures." Testimony of Matthew J. Flanigan, TIA President, before the Crime Subcommittee of the House Committee on the Judiciary (Oct. 23, 1997).

12 CALEA § 107(a)(2), *codified at* 47 U.S.C. § 1006(a)(2).

13 CALEA § 107(b), *codified at* 47 U.S.C. § 1006(b)(emphasis added). *See also* House Report, note 4, *supra,* at 27 ("The FCC retains control over the standards. . . . [CALEA] provides a forum at the [FCC] in the event a dispute arises over the technical requirements or standards.").

capability requirements . . . is not reasonably achievable through application of technology available within the compliance period."[14]

None of Congress' expectations has been met. The FBI did *not* publish a notice of capacity by October 1995 as CALEA mandated.[15] Indeed, as of today, over three years after CALEA was enacted, the FBI has *still* not published its capacity requirements. The FBI now promises to publish its capacity requirements in January 1998, but this publication admittedly will be incomplete because it will not cover all carriers.[16] The FBI has not even indicated when it might publish its capacity requirements for mobile satellite and paging carriers.[17]

The industry's attempt to develop technical capability standards (and, thereby, CALEA-compliant equipment) has faced similar obstacles. In early 1995, shortly after CALEA's enactment, the industry began to formulate, under the auspices of the Telecommunications Industry Association ("TIA") Subcommittee TR 45.2, a technical standard

---

14 CALEA § 107(c)(2), *codified at* 47 U.S.C. § 1006(c)(2).

15 Rather, the FBI waited a full year before even commencing its capacity proceeding. *See First Notice of Capacity,* 60 Fed. Reg. 53643 (Oct. 16, 1995). This proposal — presented as a percent of engineered capacity — was roundly criticized for its excess, so the FBI released a revised capability proposal 15 months later. *See Second Notice of Capacity,* 62 Fed. Reg. 1902 (Jan. 14, 1997). Although federal and state law enforcement agencies conducted a total of only 306 Title III wiretaps in 1996 (excluding pen register and trap/trace interceptions), the FBI proposes in this *Second Notice* that the industry be prepared to conduct *simultaneously* as many as 20,100 taps of all kinds.

16 The FBI has stated that its capacity requirements published in January 1998 will not address certain carriers, such as mobile satellite and paging. *See Implementation of Section 104 of CALEA, Second Notice of Capacity,* 62 Fed. Reg. 1902, 1904 (Jan. 14, 1997). *See also* discussion, *infra*, at 15-18.

17 Congress did provide a capacity "safe harbor" for industry by giving carriers three years to meet the FBI's capacity requirements *if* the FBI agrees to reimburse carriers for the costs of adding the capacity the FBI specifies. *See* 47 U.S.C. §§ 1003(b) and (e).

to implement CALEA's capability requirements. By October 1995, within one year of CALEA's enactment, the industry produced a draft standard of over 170 pages in length.

The FBI attended TR 45.2's numerous meetings, but reportedly provided no significant technical contributions or assistance. Instead, in June 1996 the FBI submitted to TIA an entirely different proposal — an Electronic Surveillance Interface ("ESI") document — as its preferred standard.[18] This FBI action resulted in considerable delay as TR45.2 attempted to reconcile — line by line — the inconsistent ESI with PN-3580. Nevertheless, the industry did integrate many of ESI's recommended requirements into its PN-3580.[19]

The industry submitted its revised standard proposal, SP-3580, for an ANSI (American National Standards Institute) ballot in March 1997.[20] At the recommendation of the FBI, which characterized SP-3580 as a "disaster," all participating law enforcement agencies voted against SP-3580, which prevented the document from becoming an industry standard.[21] Law enforcement's problem with SP-3580 was not the substance of the standards proposal, but

---

18 Among other things, ESI demanded interception and delivery of information within 500 milliseconds — several times faster than some current switching technologies react to dialed digits.

19 AirTouch notes that some of these additional requirements *were not* mandated by CALEA but were included in an effort to reach a consensus standard.

20 At about this same time, the FBI took the unprecedented step of attempting to have TIA's ANSI accreditation revoked. Had the FBI been successful, TIA would have lost not just its ability to issue SP-3580 but its ability to issue any ANSI-related standards, which could have seriously jeopardized the continued interoperability of the public switched network.

21 34 of the 65 ballots received on SP-3580 were from state and local law enforcement agencies which had not previously participated in the standards process. Twenty-eight of these "no" votes were identical, using the same 74-page statement of opposition as the FBI submitted.

rather that, in its opinion, the proposal was incomplete because it did not include additional capabilities which it demanded.[22]

The TR45.2 Subcommittee thereafter revised its SP-3580 proposal based upon the comments received, and SP-3580A was then submitted for an ANSI vote in late July or August, 1997. The same result occurred when the vote closed in November: law enforcement agencies uniformly opposed the proposed standard because, they argued, it was incomplete.[23] (It should also be noted that during the balloting period, privacy rights organizations began to contend that the industry's SP-3580 proposal had gone too far and unlawfully implicated consumers' privacy rights.[24] Also during the balloting period, and while the FBI was lobbying state and local law enforcement agencies to vote "no" on the industry proposal, the FBI testified before Congress that it "continues to work with industry on many fronts with the objective of moving forward on CALEA's capability assistance requirements."[25])

---

22 *But see* House Report, *supra,* note 4 at 22-23 ("The FBI Director testified that the legislation was intended to *preserve the status quo*, and that it was intended to provide law enforcement *no more and no less access to information than it had in the past. The Committee urges against overbroad interpretation of the requirements. . . . The Committee expects industry, law enforcement and the FCC to narrowly interpret the* [*capability*] *requirements.*") (emphasis added).

23 In response to this second ballot, 186 law enforcement agencies voted "no" while the 26 industry ballots voted "yes."

24 *See* Comments on Petition for Rulemaking of the Center for Democracy and Technology and the Electronic Frontier Foundation (Response to July 16, 1997 Petition of the Cellular Telecommunications Industry Association), *In the Matter of Implementation of Section 103 of the Communications Assistance for Law Enforcement Act* (Aug. 11, 1997).

25 Statement of H. Michael Warren, FBI Section Chief, Information Resources Division, before the Subcommittee on Crime, House Committee on the Judiciary (Oct. 23, 1997).

It again bears emphasis that the FBI twice vetoed the industry standards proposal even though it *agrees* that the proposal meets CALEA's requirements. This fact is evident from the following recent exchange between the Chairman of the House Subcommittee on Crime and the FBI section chief responsible for CALEA implementation:

> Chairman McCollum: "Does that [industry] proposal meet the standard of the act as opposed to what you want?"
>
> Michael Warren: "It does."[26]

Mr. Warren's response illustrates the problem the industry has been having with the FBI. Congress made clear that CALEA is "intended to preserve the status quo, [and] that it [is] intended to provide law enforcement no more and no less access to information than it had in the past."[27] However, the FBI has instead taken the position that the industry is required to provide "all of the functionality" which the FBI determines is necessary "to satisfy evidentiary needs dictated by law and the courts" — whether or not the functionality is specified in CALEA.[28]

---

26 *PCS Week,* "Congress Says FBI Is Trying to Exceed Authority with CALEA," Vol. 8, No. 45 (Nov. 5, 1997)' *Communications Today,* "Congress Says FBI Is Trying to Exceed Authority with CALEA" (Oct. 24, 1997).

27 House Report, *supra,* note 4 at 22.

28 *FBI, CALEA Implementation Plan,* submitted to the House and Senate Committees on the Judiciary and Appropriations (March 3, 1997). The FBI's reluctance to acknowledge the statutory capability standard is perhaps most graphically illustrated by the dispute over so-called location information, which identifies the physical location of the subject. The FBI has taken the position from the outset that CMRS providers are required to provide location information — even though CALEA expressly *precludes* such information. *See* 47 U.S.C. § 1002(a)(2)(B) ("[C]all identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number.")); House Report at 22. After the FBI refused to modify its position, the industry, as a compromise, agreed to provide the location of the serving cell site at the beginning and end of the intercepted call, and it included this capability in its standards proposal. The FBI believes this

(continued...)

In any event, realizing that law enforcement would likely veto SP-3580A, the industry decided to place the standard — now under the number, J-STD-025 — on an alternative track permitting the industry to consider whether the proposal standard should be adopted as a TIA "interim" (and ANSI "trial use") standard.[29] Law enforcement was not permitted to vote on this "interim" standard proposal, and the industry approved it last month. TIA and Committee T1 (sponsored by the Alliance for Telecommunications Industry Solutions) published this interim/trial-use standard last week.[30] In the industry's judgment, this standard, J-STD-025, meets CALEA's requirements and, as such, operates as the "safe harbor" which Congress has established.[31]

Three facts are apparent from the foregoing. First, the FBI is over two years late in meeting its statutory mandate to publish its capacity needs — inaction that has negatively

---

28 (...continued)
compromise is unacceptable and, for their part, civil rights group now contend (with considerable force) that the industry went too far in accommodating the FBI's demands. *See* note 23 *supra.* Indeed, certain mobile satellite providers and paging carriers may never be able to provide these kinds of capabilities because of limitations imposed on their license (*e.g.*, one-way spectrum).

29 In hindsight, the industry should have pursued this course in 1995 rather than spending the intervening two years attempting to negotiate with the FBI. This would have enabled the vendor community to begin developing compliant equipment and have put the onus on the FBI to challenge before the FCC the adequacy of the industry's standard.

30 CTIA has also petitioned ANSI to ignore law enforcement objections to the industry proposal so that J-STD-025 can become a final ANSI standard. An ANSI vote on the industry petition is expected in February 1998, and it is not known whether it will be granted.

31 The FBI, while not contesting that J-STD-025 satisfies CALEA, nevertheless asserts that the standard remains deficient because it does not include everything on its "wish list." Under the procedures Congress established, the burden is now on the FBI to petition the Commission — although AirTouch notes that the issues have already been raised by CTIA's pending petition.

impacted efficient design of CALEA-compliant equipment. Second, FBI tactics have delayed publication of technical capability standards by at least 18 months. Finally and as a result, no carrier will be in a position to comply with CALEA on October 25, 1998, because the FBI's actions have precluded the industry from adopting a standard before December 1997 and, given this delay, there is not sufficient time prior to October 1998 for suppliers to modify their equipment and, then, for carriers to purchase, install, and test CALEA-compliant equipment. As the president of TIA, which represents over 600 U.S. telecommunications equipment suppliers, told Congress less than two months ago:

> The October 25, 1998 deadline is not achievable. The window of opportunity has already closed."[32]

The industry is not alone in its frustration with the FBI in this area. For example, after hearing testimony concerning CALEA implementation on October 23, 1997, Representative Barr stated, "Clearly the FBI is exceeding its authority. There's not even any question they're trying to go beyond the bounds of CALEA."[33] Although the FBI admitted during the hearing that the industry proposal it had been blocking met CALEA's requirements, it

---

[32] Testimony of Matthew J. Flanigan, TIA President, before the Crime Subcommittee of the House Committee on the Judiciary (Oct. 23, 1997). *See* House Report, *supra,* note 4 at 33. It is perhaps noteworthy that, at the time it enacted CALEA, Congress expected that the FBI would expend $500 million on CALEA implementation by the end of fiscal year 1997. However, on the third anniversary of CALEA, the FBI has yet to spend a single penny of its specified authorization — because without standards the vendor community has been unable to modify its equipment for CALEA compliance.

[33] *PCS Week,* "Congress Says FBI Is Trying to Exceed Authority With CALEA," Vol. 8, No. 45 (Nov. 5, 1997).

nonetheless refused to reassure the House Crime Subcommittee that it would not prosecute the industry for failing to meet the current October 25, 1998 compliance date.[34]

B. It Is Now Timely and Essential That the Commission Address the Issues Raised in CTIA's Petition

On July 16, 1997, in an attempt to break the stalemate with the FBI, the Cellular Telecommunications Industry Association ("CTIA") filed a rulemaking petition requesting the Commission to exercise its express statutory authority by (1) adopting the industry's then-proposed technical capability standards proposal, and (2) deferring CALEA's compliance date for two years after standards have been adopted (so vendors would have time to develop compliant equipment and carriers thereafter would have time to install this equipment).[35] The Commission declined to include these issues in this rulemaking, stating:

> Based on the ongoing nature of the standard-setting process, we conclude that it would be inappropriate at this time for us to address technical capability standards issues.[36]

However, since the Commission made this determination in October, the industry's second attempt to secure ANSI approval has been vetoed by law enforcement. Reportedly, an industry meeting with the FBI, as recently as December 5, 1997, confirms that there is no realistic possibility of breaking the stalemate.

---

34 *Id.* In addition, House Appropriations Committee member Harold Rogers was reported to have won deletion of $100 million from the FBI's budget earmarked for CALEA, the Congressman stating that he was "quite angry" by the inaction on developing industry standards. *See Communications Daily,* Capitol Hill Section (Nov. 7, 1997).

35 *In the Matter of Implementation of Section 103 of the Communications Assistance for Law Enforcement Act*, Petition for Rulemaking, CTIA Petition (July 16, 1997).

36 *CALEA NPRM* at ¶ 44.

It is time for the Commission to assume the adjudicative role Congress expected it to play in ensuring that standards are adopted in a timely fashion — standards which will help both reduce implementation costs and ensure carriers nationwide can comply with CALEA's requirements. In this regard, Congress stated unequivocally:

> The FCC retains control over standards, *** [CALEA] provides a forum at the [FCC] in the event a dispute arises over the technical requirements or standards.[37]

The industry and the FBI clearly are at a stalemate. The dispute is not over the substance of the industry standard (J-STD-025); rather, it is over capabilities *not* included in J-STD-025. It is senseless to preclude the industry from implementing CALEA capabilities on which the FBI and industry generally agree. Commission intervention is therefore necessary both to finalize the standards document where work has been completed and to address the other capability issues on which the FBI and industry cannot agree. The fact is that CALEA implementation may never be realized without the Commission's intervention.

There is a separate reason for the Commission to intervene: civil rights groups now contend that certain portions of current industry standard J-STP-0025, violate CALEA and unlawfully invade consumer privacy rights.[38] It makes no sense for consumers, the industry, or the government for industry to expend resources on capabilities which may be later determined to be unlawful. Consequently, the sooner the Commission intervenes in the capability standards

---

37 House Report, *supra,* note 4.

38 The Center for Democracy and Technology and the Electronic Frontier Foundation argue that CALEA prohibits the CMRS industry from providing law enforcement with certain location information and that the proposal standard for packet data violates CALEA (because of the difficulty of separate content and call-identifying information). *See supra,* note 23.

controversy, the sooner final standards can be approved, the sooner vendors can develop CALEA-compliant equipment, the sooner carriers can install and test necessary CALEA modifications in their networks, and the sooner carriers can discharge their statutory responsibilities under CALEA.

C. CALEA Implementation Rules Must Consider the Unique Issues Faced by Mobile Satellite and Paging Carriers

The lengthy discussions which the FBI and industry have conducted to date have focused on interception issues pertaining to traditional networks: landline and cellular/broadband PCS networks. This focus is not surprising given that the vast majority of law enforcement interceptions occur on these networks. However, the FBI has been unwilling (or unable) to address the unique CALEA implementation issues faced by other networks, including mobile satellite and paging systems. As the TIA president advised Congress recently:

> Individual companies have attempted to open dialogues with law enforcement about the status of these related technologies [*e.g.*, mobile satellite and paging] and how CALEA compliance should be managed. Unfortunately, law enforcement, in particular the FBI, has been so overwhelmed with the various issues related to cellular and PCS that they have been unable to talk about these other technologies.[39]

AirTouch below identifies some of the issues unique to each of these networks.

1. *Mobile Satellite Networks.* Telephony-based low-earth-orbit satellite networks are relatively new. For example, Globalstar expects to launch the first four satellites of its

---

[39] Testimony of Matthew J. Flanigan, TIA President, before the Crime Subcommittee of the House Committee on the Judiciary (Oct. 23, 1997).

eventual 48 satellite system in February 1998, and it anticipates that commercial service, which will focus on the rural and remote areas of the world,[40] will commence early in 1999.[41]

Globalstar will likely be subject to the capability standards which TR 45.2 has developed for broadband CMRS providers generally (J-STD-025). However, unique issues are raised when a carrier attempts to implement these standards in a satellite system covering the globe as opposed to a terrestrial-based radio system serving discrete geographic areas.

Globalstar will be using the latest technology, some of which is remains under active development. Like all new systems, capabilities will be introduced over time. For example, Globalstar's introductory service will not contain all the features specified in J-STD-025, including interception of data and short messaging. Assuming these and other capabilities can be added at reasonable cost, Globalstar will, at the appropriate time, submit a waiver petition to extend the date in which it must comply with all of CALEA's assistance capability requirements.[42]

---

40 Globalstar's service will be truly unique, and thus the capacity and capability requirements for rural wireless services provided by LECs or terrestrial-based CMRS systems may be only generally applicable to Globalstar.

41 The Globalstar system is unique in that its satellites will not directly connect one user to another, but will rather connect a user to one of Globalstar's gateways, which will be connected to the public switched network. Globalstar's handsets will be dual-mode cellular/satellite compatible. Its system is being designed so that a customer's telecommunications ordinarily will be handled by a local cellular carrier when available, with satellite service generally used when the customer is located in areas where cellular service is not available.

42 Section 107(c) of CALEA authorizes carriers to request extensions of time of the statute's capability requirements if compliance "is not reasonably achievable through application of technology available within the compliance period." 47 U.S.C. § 1006(c)(2). The Commission has noted that such petitions may be filed up through October 24, 1998. *See CALEA NPRM* at ¶ 49. If certain capabilities cannot be

(continued...)

The FBI has not been ready to address the unique implementation issues pertaining to the mobile satellite service industry, as evidenced by its decision not to include capacity requirements for this industry in its upcoming notice of capacity. However, when the FBI is ready to talk, Globalstar is committed to working with the FBI, as well as other law enforcement agencies, to ensure that its system accommodates law enforcement and privacy requirements.

2. *Paging Networks.* The paging industry has accommodated law enforcement's interception needs for some time. AirTouch Paging, for example, upon receipt of a valid court order, provides law enforcement with a "clone" pager. Under this arrangement, the agency in question can receive simultaneously the same messages received by the paging customer (the subject of the subpoena) and at whatever location the agency chooses, as the "clone" pager is portable. This long-standing practice has worked well, and it is AirTouch's understanding that law enforcement agencies continue to be satisfied with the arrangement.[43]

AirTouch believes that its current practice of providing a "clone" pager meets both law enforcement's needs and CALEA's capability requirements. After all, Congress has

---

[42] (...continued)
implemented at reasonable cost, Globalstar may instead file a petition pursuant to Section 109 of CALEA. *See* 47 U.S.C. § 1008(b).

[43] Congress is currently considering legislation which would clarify the standards under which law enforcement can obtain a court order for a clone pager. *See* Clone Pager Authorization Act of 1996, S. 170, 105th Cong., 1st Sess. This bill passed the Senate on November 8, 1997, and it has been referred to the House for its consideration.

made clear that CALEA is intended "to provide law enforcement no more and no less access to information than it had in the past."[44]

The Commission should be aware that the paging industry has not had an opportunity to confirm this assumption with the FBI. CALEA implementation issues unique to paging systems have not, to AirTouch's knowledge, been addressed in either the TR 45.2 deliberations or in the discussions between the FBI and the industry — which is perhaps understandable given that paging interceptions constitute such a small percentage of total interceptions. Indeed, the FBI's notice of capacity expected for release next month will not include the FBI's capacity requirements for paging carriers, and it is not now known when the FBI will be prepared to address paging implementation issues.[45] However, AirTouch Paging stands ready to work with the FBI once it is ready to address issues unique to paging.[46]

---

44 *See* House Report, *supra,* note 4 at 22-23. For example, one-way paging systems, will never have the capability to determine a subscriber's whereabouts — even if CALEA permitted law enforcement to receive location information. In addition, traditional wiretapping makes no sense for paging because a cloned pager provides the same information in a timely (indeed, simultaneous) fashion.

45 Indeed, given the FBI's delay in identifying additional capabilities for paging systems, it would be especially appropriate for the Commission to grant the paging industry an open-ended waiver from any additional CALEA requirements.

46 Law enforcement agencies should be forewarned that it will be difficult for paging carriers to provide capabilities not made available today. For example, AirTouch Paging cannot currently provide law enforcement with access to its customers' voice mailbox because its customers have the flexibility to devise (and change) their own custom passwords — without the intervention or even knowledge of AirTouch. Similarly, the number of the calling party is not available without SS7 interconnection, but paging carriers rarely use SS7. While LECs make the billing number (or ANI) available with Type 2 interconnection, they do not make this date available with Type 1 interconnection, the predominant interconnection used by AirTouch. Moreover, with respect to Type 2, AirTouch's switches are not currently configured to acknowledge billing data.

II. Many of the Compliance/Recordkeeping Proposals Are Unnecessary and Cannot Be Justified Under the Paperwork Reduction Act

Congress has directed the Commission to "prescribe such rules as are necessary to implement the requirements of [CALEA]."[47] However, Congress has also directed the Commission to impose only those paperwork regulations that are "necessary" and have "practical utility."[48] AirTouch demonstrates below that many of the proposed compliance/recordkeeping proposals, apparently made at the recommendation of the FBI,[49] are not necessary, would have no practical utility, and would have the result of imposing needless costs on carriers — costs which would be passed through to the consuming public.

Two general observations bear emphasis at the outset. First, even without new Commission regulations, carriers and their employees have ample incentive to ensure they comply with CALEA and protect the privacy of their customers' communications. This incentive is created by existing legal obligations and the penalties which can be imposed for ignoring these obligations. For example, carriers and their employees not complying with the interception laws may be subjected to criminal prosecution,[50] to a civil damages action,[51] to a Commission forfeiture action,[52] *and* to a law enforcement action which could result in fines of up

---

47 47 U.S.C. § 229(a).

48 Paperwork Reduction Act of 1995, 104 Pub. Law 13, 109 Stat. 163, *codified at* 44 U.S.C. § 3506(c)(2)(A).

49 *See CALEA NPRM* at ¶ 24.

50 *See* 28 U.S.C. § 2511(1).

51 *See* 28 U.S.C. § 2520.

52 *See* 47 C.F.R. § 1.80; *see also* 47 U.S.C. § 503(b); *CALEA NPRM* at ¶ 37.

to $10,000 per day.[53] Further, market forces provide an equally compelling incentive; any carrier ignoring its customers' privacy rights may find it difficult to remain in business. Given these powerful incentives, coupled with the requirements of the Paperwork Reduction Act and the fact that the industry has been performing authorized interceptions for nearly 30 years without administrative regulations, the Commission should exercise great care before imposing any new compliance or recordkeeping requirement on carriers — and on competitive carriers in particular.

Second, CMRS providers in particular are undergoing dramatic growth. In the three short years since CALEA was enacted, the number of CMRS customers has more than tripled (from 16 million to over 50 million). Not surprisingly, the number of interceptions performed on CMRS networks has grown dramatically as well.[54] This means that any compliance/record-keeping regulations which the Commission adopts will have an increasingly disproportionate impact on the CMRS industry — a competitive industry which can ill-afford new, regulatory-imposed costs not required by prudent business practices.

A. An Annual Affidavit of Designated Employees, Rather than an Affidavit-per Interception Is Adequate

The FBI proposes that each employee involved in an interception prepare and execute an affidavit each time he or she performs an interception, and that such an affidavit be

---

53 *See* 18 U.S.C. § 2522.

54 CMRS taps accounted for less than 25% of all federal taps conducts in 1993. According to the government's 1996 wiretap report, CMRS taps now exceed 34% of all federal taps conducted.

prepared "not later than 48 hours from the time each interception begins."[55] This "affidavit-per-interception" proposal is not necessary, and governmental objectives can be adequately achieved by allowing designated employees to execute annual, blanket affidavits.

AirTouch, like most carriers, has designated specific employees to implement authorized interceptions. Such an arrangement is not only efficient for law enforcement and carriers alike, but it also gives designated employees an opportunity to become more knowledgeable about the limits of authorized interceptions. In these circumstances, no purpose would be served by requiring designated employees to prepare and execute an affidavit with each interception — even assuming such an affidavit could be prepared within 48 hours.[56] An annual certification requirement should be more than sufficient.

B. The Proposed Interception Records Are More Detailed Than They Need to Be

The FBI proposes that carriers make a record of each interception and that each interception record contain the following seven items of information:

1. The telephone number (or circuit number) involved;
2. The date and time the interception started;
3. The date and time the interception stopped;

---

55 *See CALEA NPRM* at ¶ 31; Proposed Rule 64.1704(a).

56 In this regard, employees receiving a court order on a Friday afternoon or evening may have difficulty meeting the 48-hour proposal. In addition, at many of its network locations AirTouch does not have a notary public on site, so an affidavit requirement would require the employee to leave his or her job responsibilities in an attempt to locate a notary. Finally, it is not apparent how consumer privacy interests are protected when interception affidavits are notarized by persons not even employed by the carrier.

4. The identity of the law enforcement officer presenting the authorization;

5. The name of the judge or prosecuting attorney signing the authorization;

6. The type of interception; and

7. The names of all carrier personnel involved in "performing, supervising, and internally authorizing, the interception, and the name of those who possess knowledge of the interception."[57]

Much of this information — including items (1), (2), (3), (5), and (6) — is already generally contained in the court order.[58] No purpose would be served by having carries duplicate information that already exists and which law enforcement will retain. Moreover, the Paperwork Reduction Act specifically provides that agencies should avoid imposing recordkeeping requirements which are "unnecessarily duplicative of information otherwise reasonable accessible.[59]

In addition, it is not apparent why carriers should be required to record the identity of the officer presenting the court order (item (4)) — even assuming such information exists.[60] If any law enforcement identity information is useful, it would be the identity of the

---

57 *See CALEA NPRM* at ¶ 31; Proposed Rule 64.1704(a).

58 *See* 18 U.S.C. § 2518(4). In addition, although the court order specifies the outside time limits of an authorized interception, carriers obviously do not know when law enforcement actually intercepts the target's communications.

59 44 U.S.C. § 3506(c)(3)(B).

60 Because law enforcement and AirTouch's designated employees have developed such a good working relationship, law enforcement personnel often "fax" court orders to AirTouch's designated employees — preventing AirTouch from identifying the particular officer "presenting" the order.

officer seeking an interception. However, this information is contained in the application for a court order,[61] and no purpose would be served by having carriers duplicate it. Besides, if the FBI believes it is important to record the identity of the officer presenting a court order to a carrier, law enforcement agencies are capable of recording this information directly.

Likewise, no purpose would be served by requiring carriers, each time an interception is performed, to record "the names of all . . . personnel involved in performing, supervising, and internally authorizing, the inception, and the names of those who possessed knowledge of the interception."[62] The number of carrier employees authorized to effectuate interceptions is relatively small, and the same group of designated employees handle all interceptions. This proposal would therefore require carriers to undertake unnecessary additional work by repeating with each interception a list of the same employees.[63]

The Commission should also clarify that proposed rules 64.1404(c) and (c), requiring maintenance of a "separate record . . . of the identities of third parties to which disclosure of call-identifying information is made," excludes communications between designated employees and the officers of the law enforcement agency obtaining the court order. With this clarification, AirTouch does not object to these proposed rules — although the need for the rules is not apparent because disclosure of interception information to third parties is

---

61 *See* 18 U.S.C. § 2518(1).

62 Proposed Rule 64.1704(a)(7).

63 Even more inappropriate — and unnecessary — is the *NPRM* proposal that designated employees record not only their names with each interception, but also their "respective positions within the telecommunications carrier." *CALEA NPRM* at ¶ 31.